Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	

To: The Commission

REPLY COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION F/K/A THE CONSUMER ELECTRONICS ASSOCIATION

The Consumer Technology Association ("CTA")[1] respectfully submits these reply comments in response to the Federal Communications Commission's ("Commission" or "FCC") *Notice of Proposed Rulemaking* ("*Notice*") in the above-captioned proceeding. The record clearly does not support the onerous and prescriptive rules proposed in the *Notice*, nor could it; a prescriptive approach to privacy and data security that treats all data the same, regardless of the sensitivity of such data, would fail to align with consumer expectations and chill innovation, all without a corresponding benefit to consumer privacy. If the Commission acts in this proceeding, it should adopt a principles-based approach – consistent with the approach of the Federal Trade

[1] The Consumer Technology Association ("CTA")™ is the trade association representing the $287 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development, and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technology. Profits from CES are reinvested into CTA's industry services.

Commission ("FTC") – that recognizes that some types of personally identifiable information are more sensitive than others.

I. A BROAD ARRAY OF STAKEHOLDERS HAVE IDENTIFIED FUNDAMENTAL FLAWS IN THE PROPOSED RULES

As detailed in CTA's initial comments, the Commission's proposed privacy requirements for broadband internet access service ("BIAS") providers go beyond the Commission's limited legal authority and would harm consumers, undermine their trust in the internet ecosystem, and chill innovation – all without creating much benefit for consumers' privacy.[2] In particular, CTA agrees with the many other commenters who note that the Commission's failure to relate requirements to the sensitivity of the underlying data is one of the fundamental flaws in its proposal.

As CTA and others have noted, the Commission's proposed rules are not only onerous and prescriptive, but also inconsistent with the robust framework of the FTC Act, state unfair or deceptive acts or practices laws, self-regulatory programs, and other laws and guidelines around which many companies operating in the internet ecosystem have structured their privacy and data security programs – and which have served consumers well.[3] This inconsistency and departure from consumers' expectations would undermine the trust that is essential to consumers' adoption of innovative internet-based services, as well as related devices and software. For example, few things would be more jarring to consumers than to learn that an ISP must treat information concerning a consumer's use of a wellness-related wearable device –

[2] *See generally* CTA Comments.

[3] *See* FTC Staff Comment at 3-6 (summarizing FTC privacy enforcement history).

information which CTA members view as sensitive and deserving of special handling[4] – that the ISP carries on its network in exactly the same manner as that ISP must treat the consumer's name. But under the proposed rules, that is precisely what would happen once data hits a BIAS provider's network. Rules that clash with consumers' expectations in such a stark fashion provide a recipe for undermining consumer trust.

Indeed, the record is replete with comments from a range of stakeholders who have concluded that this approach would be a big step in the wrong direction.[5] Among the critics of the Commission's proposed rules is the consumer protection staff of the nation's leading

---

[4] *See generally* Consumer Technology Association, *Guiding Principles on the Privacy and Security of Personal Wellness Data* (Oct. 20, 2015), http://www.cta.tech/healthprivacy.

[5] *See, e.g.*, American Cable Association ("ACA") Comments at 31 ("[t]he Commission's proposal flips the FTC's successful approach on its head, defaulting to an 'opt-in' framework that is out of step with the market and customer expectations"); Association of National Advertisers ("ANA") Comments at 24, 27-29 ("the Commission's proposed rules ignore key differences in consumer expectations for sensitive and less-sensitive information"); AT&T Comments at 56-58 ("the proposed regulations would generate consumer confusion about exactly what is, and what is not, subject to particular privacy protections"); CenturyLink Comments at 3-4 (the rules would "perplex consumers" and "then compound this confusion by inundating customers with notifications that are not relevant to their needs"); Competitive Carriers Association ("CCA") Comments at 4, 8 (the proposed rules are "significantly more restrictive than other well-known privacy regimes already in place, and are applicable to a much broader set of data, which would lead to consumer confusion and ultimately fail to adequately meet consumer expectations"); Consumers' Research Comments at 7-9 (there has been no "sea change in consumer behavior or expectations"; the Commission "should not impose on the Internet its own normative view of consumers' privacy preferences"); CTIA Comments at 119-136 (under effective privacy regimes, heightened protection is required only for heightened risk; the Commission's proposal is "untethered" from consumer expectations); Information Accountability Foundation Comments at 2-4 (emphasizing the importance that the Commission's rules "be in line with and interoperable with other International laws and market expectations"); Information Technology Industry Council Comments at 7-8 (the Commission should not promulgate rules that "are inconsistent with consumer expectations" or "that are inconsistent with existing privacy frameworks and enforcement regimes"); National Cable & Telecommunications Association Comments at 73 (the Commission's proposal is "wholly at odds with the FTC and White House frameworks, as well as customer expectations"); ViaSat, Inc. Comments at 6 (an opt-in regime would not be "consistent with customers' expectations").

consumer privacy enforcement agency, the FTC.[6] The FTC's decades of consumer privacy enforcement and policy experience make the views of its staff worthy of careful consideration.[7] Although it is measured in its language, the FTC Staff Comment points out some deep flaws in the proposed rules.[8]

Perhaps the most central of these flaws lies in the approval, or consumer choice, elements of the proposed rules,[9] which draw no distinctions according to how sensitive so-called "customer proprietary information" is. Instead, the proposed rules "generally track[] the precedent laid out years ago in the FCC's existing CPNI Rule,"[10] but "this approach does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data."[11] FTC staff concludes that the FCC's approach "could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful."[12] This criticism identifies a structural flaw in the FCC's

---

[6] *See generally* Staff of FTC Bureau of Consumer Protection Comment ("FTC Staff Comment").

[7] *See* FTC Staff Comment at 3-6 (describing the FTC's consumer privacy program); *see also Notice* ¶ 2 (noting the FTC's "important leadership"); *id.* ¶ 4 (The *Notice* "looks to learnings from the FTC and other privacy regimes to provide complementary guidance."). As CTA and others noted, the proposals in the *Notice* substantially depart from the FTC's privacy approach, and are far from complementary. *See, e.g.,* CTA Comments at 11-13.

[8] FTC Staff Comment at 19-20.

[9] Customer Approval Requirements (proposed 47 CFR § 64.7002).

[10] FTC Staff Comment at 22.

[11] *Id.*

[12] *Id.*; *see also* Separate Statement of FTC Commissioner Maureen Ohlhausen at 3 ("If a regulation imposes defaults that do not match consumer preferences, it imposes costs on consumers without improving consumer outcomes. The burdens imposed by a broad opt-in requirement may also have negative effects on innovation and growth.").

proposed rules; it is not just an assessment of how the proposed rules would play out in practice. Many others have emphasized the risks of ignoring data sensitivity.[13]

II. A WORKABLE FRAMEWORK MUST BE BASED ON A DISTINCTION BETWEEN SENSITIVE AND NON-SENSITIVE INFORMATION

Although CTA does not agree in every particular with how the FTC staff would define "sensitive information," CTA embraces the overarching concept that distinguishing sensitive information from other kinds of personal information is the appropriate starting point for any legal framework that seeks to protect consumer privacy while promoting innovation. The "sensitive" information designation, and the heightened privacy and security protections that

[13] *See, e.g.*, ANA Comments at 23-24 (the "Commission's proposed rules impose restrictions … without regard to the variation in sensitivity," which "would have particularly drastic competitive consequences for advertising"); CenturyLink Comments at 16 ("applying any proposed requirements to all [customer proprietary information] without adequately taking into account the sensitivity of any given category of information is bad policy and inconsistent with consumer expectations"); Cincinnati Bell Telephone Company LLC Comments at 10 (it is unwise that the proposed rules "are not tied to the sensitivity of the information being used, but rather to the nature of its use"); INCOMPAS Comments at 12 ("any opt-in requirements should be reserved for the use of sensitive data in a way that would surprise consumers"); Internet Commerce Coalition Comments at 9-10 (the Commission should "define obligations by virtue of the sensitivity of the information"); Former FTC Chairman Jon Leibowitz Comments at 9 (the Commission's proposal is overbroad; the agency should not "require an opt-in without regard to the sensitivity of the data used in tailoring the advertising"); Professor Laurence H. Tribe Comments at 5 ("The proposal is not keyed to the sensitivity of consumer information, unlike the FTC's existing regulatory scheme. The FCC's proposal uses the same blunderbuss, speech-suppressing approach for all types of information."); *see also See* Letter from American Cable Association et al. to Tom Wheeler, Chairman, FCC (Feb. 11, 2016), *available at* http://www.ctia.org/docs/default-source/fcc-filings/021116-privacy-letter.pdf; Letter from American Cable Association et al. to Tom Wheeler, Chairman, FCC (Mar. 1, 2016), *available at* https://www.ncta.com/sites/prod/files/Letter-PrivacyPrinciples-3-1-16.pdf. *See also* Debbie Matties, A Rethink Is Needed on the FCC's Broadband Privacy Proposal (June 8, 2016), available at http://www.ctialatest.org/2016/06/08/rethink-fcc-proposed-broadband-privacy-rules/ (expressing the views of CTA, CTIA, Mobile Future, USTelecom and Wireless Internet Service Providers Association).

should accompany such information, should be reserved for a small subset of personally identifiable information.[14]

This is not hypothetical support, but demonstrable commitment to providing the right amount of protection for the right type of data. CTA has put this view into concrete principles in the context of health and wellness devices that effectively balance innovation and evolving technology with consumers' need for and expectations of privacy. Many CTA members produce wearable devices or provide data analytics services that collect and use personal wellness data, such as a consumer's heart rate or activity level. Harnessing this data is helping consumers improve their well-being, empowering them to lead healthier lives, and bringing benefits to society as a whole through exciting new research. CTA also recognizes that personal wellness data may be sensitive. To help foster appropriate protections across the health and fitness wearable ecosystem, CTA developed voluntary best practices regarding security, notice, use, disclosure, and review and correction. Some of these protections, such as review, correction, and deletion, go beyond what the Commission's proposed rules would require – an appropriate outcome for a well-defined, sensitive subset of personally identifiable information.

More generally, CTA's principles demonstrate how privacy protections for sensitive data can meet consumers' expectations and promote innovation. The principles recommend that, in most circumstances, companies should seek consumers' affirmative consent before transferring personal wellness data to unaffiliated third parties. A broad fairness principle recommends that companies refrain from knowingly using or disclosing personal wellness data in a manner likely to be unjust or prejudicial to consumers' eligibility for or access to employment, healthcare,

[14] CTA reiterates, however, that the Commission's authority to address privacy and data security is limited to telecommunications carriers' use and protection of customer proprietary network information in their provision of telecommunications services. *See* CTA Comments at 4-7.

financial products or services, credit, housing, or insurance. For first-party advertising, the principles recommend allowing consumers to opt out. For other uses, such as the fitness tracking and health data analytics services for which millions of consumers buy wellness-related wearable devices, companies may infer consent to use personal wellness data while also providing consumers with the ability to review, correct, and delete the data.

These principles strike the right balance: they protect consumers from unexpected uses by giving them appropriate control over wellness data about them while enabling companies to use the data to deliver the innovative services that consumers want.[15]

III. CONCLUSION

If the Commission acts in this proceeding, it should only adopt a principles-based approach that is consistent with the FTC's privacy framework.[16] Any rules must begin with a

[15] Critically, CTA members developed these principles through voluntary, self-regulatory efforts rather than government mandate. As CTA and others have noted in this proceeding, industry players across the internet ecosystem have worked for years to devise privacy best practices that protect consumers while remaining nimble enough to adjust to evolving consumer expectations and flexible enough to allow innovation. *See* CTA Comments at 12-13; *see also, e.g.*, ACA Comments at iv, 39-42 ("[u]nlike the Commission's proposal" the industry proposal "will promote consistency across the entire Internet ecosystem, flexibility consistent with provider needs and consumer expectations, and innovation to drive the virtuous circle"); AT&T Comments at 34 ("AT&T supports the substantive principles outlined in the Industry Framework, which would subject ISPs to a regime similar to the FTC's"); Cincinnati Bell Comments at 3 (urging "the Commission to adopt that proposal as its approach to privacy protection for BIAS rather than the one put forth in the NPRM"); CCA Comments at 5-9 (the industry framework is "flexible, transparent, and consistent with consumer expectations and the public interest," whereas the Commission's proposals "conflict with existing and developing privacy regimes"); Electronic Transactions Association Comments at 8 (recommending that, if the Commission decides to go forward with its current efforts, it should rely on the industry framework, which is "consistent with the approach the FTC successfully implemented before reclassification to ensure that the data privacy and security practices of broadband providers were transparent, fair and non-deceptive"); WISPA Comments at 11 ("the Industry Framework will enable the Commission and the FTC to achieve the goals stated in their Memorandum of Understanding by avoiding 'duplicative, redundant or inconsistent oversight' and consistent policies and basis for enforcement").

recognition that some types of personally identifiable information are more sensitive than others. Unless the Commission makes this fundamental change to its proposals, the agency will remain far out of step with the needs of businesses, the expectations of consumers, and the sensible framework developed by the FTC over its decades of consumer privacy enforcement experience.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION F/K/A CONSUMER ELECTRONICS ASSOCIATION

By: */s/*

Julie M. Kearney
Vice President, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

July 6, 2016

[16] *See* CTA Comments at 13.